UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/954,976	09/18/2001	Surendra N. Naidoo	4017-03001	8803

30652 7590 11/08/2010

CONLEY ROSE, P.C.
5601 GRANITE PARKWAY, SUITE 750
PLANO, TX 75024

EXAMINER	
VO, TUNG T	

ART UNIT	PAPER NUMBER
2483	

MAIL DATE	DELIVERY MODE
11/08/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/954,976
Filing Date: September 18, 2001
Appellant(s): NAIDOO ET AL.

Clint R. Stuart Reg. No. 48,859
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 09/08/2010 appealing from the Office action mailed 03/09/2010.

(1) Real Party in Interest

The examiner has no comment on the statement, or lack of statement, identifying by name the real party in interest in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The following is a list of claims that are rejected and pending in the application:

1, 3-24, 26-31, 47-52, and 57-61.

(4) Status of Amendments After Final

The examiner has no comment on the appellant's statement of the status of amendments after final rejection contained in the brief.

(5) Summary of Claimed Subject Matter

The examiner has no comment on the summary of claimed subject matter contained in the brief.

(6) Grounds of Rejection to be Reviewed on Appeal

The examiner has no comment on the appellant's statement of the grounds of rejection to be reviewed on appeal. Every ground of rejection set forth in the Office action from which the appeal is taken (as modified by any advisory actions) is being maintained by the examiner except for the grounds of rejection (if any) listed under the subheading "WITHDRAWN

REJECTIONS." New grounds of rejection (if any) are provided under the subheading "NEW GROUNDS OF REJECTION."

(7) Claims Appendix

The examiner has no comment on the copy of the appealed claims contained in the Appendix to the appellant's brief.

(8) Evidence Relied Upon

6,442,241	Tsumpes	08-2002
6,504,479	Lemons et al.	01-2003
6,826,173	Kung et al.	11-2004
6,667,688	Mennard et al.	12-2003
6,400,265	Saylor et al.	06-2002

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1 and 3-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tsumpes (US 6,442,241 B1).

Re claim 1, Tsumpes teaches a security system (fig. 1) comprising: a security gateway *(12 of fig. 1, the controller is considered as a security gateway)* located at a premises *(11of fig. 1, sensors are obviously alarm and video systems)*, wherein the security gateway (12 of fig. 1) is operable to detect an alarm condition *(col. 6, lines 32-37)* and to record video of at least a portion of the premises relating to the alarm condition, said video hereinafter referred to as an Alarm Video *(Alarm inputs, 11 of fig. 1, wherein alarm inputs 11 are video that would obviously be considered as alarm video; col. 8, lines 45-50, note the digital data packet DDP and wireless or Internet communication network also enables the present system to provide video and/or audio transmissions from the monitored device or premises to the central monitoring station due to the bandwidth capabilities of most digital data packet networks)*;

a security system server (13 of fig. 1) operatively coupled to the security gateway through a first network (19 of fig. 1) and a second network (20 of fig. 1);

wherein the security gateway*(12of fig. 1, the controller is considered as a security gateway)* is to transfer ***alarm information consisting of*** the Alarm Video (e.g. 11 of fig. 1, note *wherein alarm inputs 11 are video)* the and ***a first notification of the alarm condition (e.g. DDP includes notification of the alarm condition)*** to the security system server in substantially real time through only the first network *(col. 4, line 64-col. 5, line 33, transmission of notification alarms between the security gateway and the security system server, 12 and 13 of fig. 1; col. 8, lines 45-50, note the digital data packet DDP and wireless or Internet communication network also enables the present system to provide video and/or audio transmissions from the monitored device or premises to the central monitoring station due to the bandwidth capabilities of most digital data packet networks, therefore one skill in the art would*

used this suggestion to design the system for transmitting the video through only the first network, 19 of fig. 1);

wherein the security gateway (12 of fig. 1) is further configured to ***transfer to*** the security system server ***a second notification*** of the alarm condition (Another input 11 has a second notification of the alarm condition) through the ***second*** network (19 and 20 of fig. 1, col. 5, lines 19-23, note DDP is transmitted via the wireless transceiver and radio frequency RF transceiver), and

wherein the security system server thereby receives the Alarm Video, the first notification of the alarm condition, and the second notification of the alarm condition from the security gateway (the central monitoring station security system server receives one or more alarms from the premises, col. 1, lines 15-25, and Digital Data Packet that include the Alarm Video, col. 8, lines 45-50);

transmitting the second notification of the alarm condition through second network (20 of fig. 1) substantially simultaneously with transferring the alarm information to the security server through the first network (col.8, lines 18-23)

Note Tsumpes discloses one of the major benefits of the present pre-programmed and automated ***parallel*** and ***redundant*** contact and notification system and method is that it provides expeditious and efficient handling of time sensitive events and significantly reduces response time in emergency situations (col. 8, lines 18-23). The communications networks are in parallel that would obviously transmit the notifications simultaneously, and the communications networks are in redundant that would obviously transmit the notification via the first communication network or the second communication network as back-up network, or

redundantly transmit the notification through fist and second networks substantially at the same time.

The above disclosure fairly suggests the communications networks (19 and 20 of fig. 1) are in parallel and redundant for substantially simultaneously transmitting notification of the alarm condition with transferring the alarm information to the central monitoring system (13 o fig. 1). Doing so would provide many benefits including reduction of false alarms and false dispatches.

Re claims 3-12, Tsumpes further teaches the first network is an IP network, an Ethernet-based network, Internet, a frame relay network, a hybrid-fiber coaxial network, a fiber-optic network, a DSL network, an ATM network, a high-speed fixed wireless network, a high-speed mobile communications network (DDP, DMTF, WIRELESS of fig. 1; One skill in the art would use the well known and suitable network that are available in the market).

Re claim 13, Tsumpes further teaches the second network comprises a public switched telephone network, a fixed wireless network, a mobile communications network (DDP of fig. 1).

Re claim 16, Tsumpes further teaches wherein the security gateway is further operable to record audio from at least a portion of the premises relating to the alarm condition, said audio referred to hereinafter as Alarm Audio, and wherein the security gateway is further configured to transmit said Alarm Audio to the security system server through the second network in substantially real time (col. 8, lines 45-50).

Re claims 17 and 18, Tsumpes further teaches wherein the security system server is configured to provide notification of the alarm condition to a public safety agency (user or further security services fig. 1).

Re claim 19, Tsumpes further teaches wherein the security gateway is further operable to record audio from at least a portion of the premises relating to the alarm condition, said audio referred to hereinafter as Alarm Audio, and wherein the security gateway is further configured to transmit said Alarm Audio to the security system server through the first network in substantially real time (col. 8, lines 45-50).

3. Claims 47-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tsumpes (US 6,442,241 B1) in view of unpatentable over Lemons (US 6,504,479).

Re claims 47-49, Tsumpes does not particularly teach wherein the security gateway is further configured to detect if connectivity with the security system server through the first network is lost and transfer to the security system server by sending a notification signal through the second network of the loss of connectivity through the first network; wherein the security gateway is further configured to transfer to the security system server in the event that connectivity with the security system server through the first network is lost while the security gateway is disarmed and the security gateway is armed before connectivity with the security system server through the first network is restored as claimed.

Re claims 47-49, Lemons teaches wherein the security gateway (12 of fig. 1) is further configured to detect if connectivity with the security system server through the first network (36 of fig. 1, note the backup communications channel, 50 of fig. 1, is connected when the first network, 36 of fig. 1, is interrupted) is lost and transfer to the security system server by sending a notification signal through the second network of the loss of connectivity through the first network (Note in case the channel 36 is broken, interrupted, or otherwise impaired, the

controller 200 is connected to the monitoring center 38 via the CTE252 and the communications channel 50, col. 9, lines 51-61); wherein the security gateway (12 of fig. 1) is further configured to transfer to the security system server (38 of fig. 1) in the event that connectivity with the security system server through the first network is lost (e.g. 36 of fig. 1, the channel 36 is interrupted, col. 9, lines 51-61) while the security gateway is disarmed (col. 5, lines 5-13) and the security gateway is armed before connectivity with the security system server through the first network is restored (note the channel 36 is protected before sending video and alarm condition to the server, 38 of fig. 1).

Taking the teachings of Tsumpes and Lemons as a whole, it would have been obvious to one of ordinary skill in the art to modify the teachings of Lemons into the security system of Tsumpes for reducing redundancies in the control of all of the systems, and provides a common communications channel for alarm reporting and exchange of information with a remote monitoring center.

4. Claims 20-24, 26-31, and 50-52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lemons (US 6,504,479) in view of Tsumpes (US 6,442,241 B1) and further in view of Kung et al. (US 6,826,173).

Re claim 20, Lemons teaches a security system (fig. 1) comprising: a security gateway (12 of fig. 1) located at a premises (12a and 12b of fig. 8),

wherein the security gateway (12 of fig. 1) is operable to detect an alarm condition and to record video of at least a portion of the premises relating to the alarm condition to form an alarm video (16, 18, 20, 22 of fig. 1; see fig. 3),

wherein the security gateway (12 of fig. 1) further comprises a network interface (14 of fig. 1, Note the connections between the components (24, 26, 28, 30, 34, 56 of fig. 1), and

wherein the network interface is configured to connect the security gateway a head-end through out a first network (col. 6, line 62-col. 7, lines 50, Note the connections between components are considered as the first network; a network is a fabric or structure of cords or wires that cross at regular intervals and are knotted or secured at the crossings, a system of lines or channels resembling a network, an interconnected or interrelated chain, group, or system, or a system of computers, peripherals, terminals, and databases connected by communications lines);

a security system server (38 of fig. 1) configured to connect to the interface (34 of fig. 1) through a second network (36 of fig. 1),

wherein the security gateway (12 and 14 of fig. 1) is configured to **transfer to** the security system server **alarm information consisting of a first notification** of the alarm condition and the Alarm Video to the security system server in substantially real time (col. 7, lines25-50) only through the second network (36 of fig.1, the alarm condition and alarm video is transmitted to the server using the network as the second network);

wherein the security gateway (12, 14 of fig. 1) is operatively coupled to the security system server (38 of fig. 1) through a third network (50 of fig. 1) for redundant transmitting the alarm condition, the security gateway being further configured to **transfer to** the security system server of the alarm condition through the third network (col. 4, line 66 through col. 5, lines 14);

wherein the security gateway is configured to transfer the alarm information to the security system server through the second network (36 of fig.1, the alarm condition and alarm video is transmitted to the server using the network as the second network).

Lemons suggests that any communications channel available (36 and 50 of fig. 1) such as a hybrid-fiber coaxial network; a fiber-optic network, an ATM network, and a high-speed mobile communications network, that connects between the gateway (12 of fig. 1) is used in the security system, so this is evidence to one skilled in the art to modify any conventional network into the security system of Lemons.

It is noted that Lemons does not particularly teach substantially simultaneously with transferring the second notification of the alarm condition to transferring the security system server through the third network, and wherein the security system server is configured to receive the Alarm Video through the second network, to receive the first notification of the alarm condition through the second network, and to receive the second notification of the alarm condition through the third network as claimed.

Tsumpes teaches simultaneously transferring the alarm to the security server (13 of fig. 1) of the alarm through the second network (19 of fig. 1) and the third network (20 of fig. 1), and wherein the security system server (13 of fig. 1) is configured to receive a notification of the alarm condition through the second network (19 of fig. 1) and to receive another notification of the alarm condition through the third network (20 of fig. 1*; note* one of the major benefits of the present pre-programmed and automated ***parallel*** and ***redundant*** contact and notification system and method is that it provides expeditious and efficient handling of time sensitive events and significantly reduces response time in emergency situations (col.8, lines 18-23). The disclosure above fairly suggests the communications networks (19 and 20 of fig. 1)are in parallel and redundant (note the communications networks are in parallel that would obviously transmit the notifications simultaneously, and the communications networks are in redundant that would

obviously transmit the notification via the first communication network or the second communication network as back-up network, or redundantly transmit the notification through fist and second networks substantially at the same time).

Therefore, taking the teachings of Lemons and Tsumpes as a whole, it would have been obvious to one of ordinary skill in the art to modify the teachings of Tsumpes, the automated parallel and redundant contact to a user notification one or more alarms, into the security system of Lemons for one of the major benefits of the automated parallel and redundant contact and notification system and method is that it provides expeditious and efficient handling of time sensitive events and significantly reduces response time in emergency situations.

The combination of Lemons and Tsumpes teaches all limitation above, except the interface of the security gateway connects to a cable head-end through the first network by a hybrid-fiber-coaxial network as claimed.

However, Kung teaches a security gateway (102 of fig. 1) connects to a cable head-end (115 of fig. 1) through a first network (112 of fig. 1) by a hybrid-fiber-coaxial network (col.5, line 44 through col. 6, line 9).

Therefore, taking the teachings of Lemons, Tsumpes, and Kung as a whole, it would have been obvious to one of ordinary skill in the art to incorporate the cable head-end (115 of fig. 1) through the first network (112 of fig. 1) by the hybrid-fiber-coaxial network (col.5, line 44 through col. 6, line 9) of Kung into the communications channel (34 and 36 of fig. 1) of the combined security of Lemons and Tsumpes for the same purpose of transmitting the alarm video and alarm condition from the security gateway to the security server. Doing so would provide improved performance and quicker response time for an individual user.

Re claims 21-24, 26-28, Lemons further teaches the first network is an IP network (a network in which transmission of information is done using IP protocol; e.g. Internet network), an Ethernet-based network (LAN), the Internet, a frame relay network (a frame relay is a telecommunication service designed for cost-efficient data transmission for intermittent traffic between local area networks (LANs) and between end-points in a wide area network (WAN); a DSL network; a high-speed fixed wireless network (36 of fig. 1; see col. 5, lines 18-23); Lemons further suggests any communications channel available (36 and 50 of fig. 1) such as a hybrid-fiber coaxial network; a fiber-optic network, an ATM network, and a high-speed mobile communications network, that connects between the gateway (12 of fig. 1) is used in the security system; and wherein the second network comprises a public switched telephone network and a fixed wireless network (col. 5, lines 25-30).

Re claim 29, Lemons further teaches wherein the security gateway is further operable to record audio from at least a portion of the premises relating to the alarm condition, said audio referred to hereinafter as alarm audio, alarm video, and wherein the security gateway is further configured to transmit said alarm audio and video to the security system server through the second network in substantially real time (102, 108, 110, 112, 114, 116, and 118 of fig. 2; alarm 144 and 160 of fig. 3).

Re claims 30 and 31, Lemons further teaches wherein the security system server is configured to provide notification of the alarm condition to a public safety agency (42, 44, 46, and 48 of fig. 1).

Re claims 50-52, Lemons further teaches wherein the security gateway (12 of fig. 1) is further configured to detect if connectivity with the security system server through the first

network (36 of fig. 1, note the backup communications channel, 50 of fig. 1, is connected when the first network, 36 of fig. 1, is interrupted) is lost and transfer to the security system server by sending a notification signal through the second network of the loss of connectivity through the first network (Note in case the channel 36 is broken, interrupted, or otherwise impaired, the controller 200 is connected to the monitoring center 38 via the CTE252 and the communications channel 50, col. 9, lines 51-61); wherein the security gateway (12 of fig. 1) is further configured to transfer to the security system server (38 of fig. 1) in the event that connectivity with the security system server through the first network is lost (e.g. 36 of fig. 1, the channel 36 is interrupted, col. 9, lines 51-61) while the security gateway is disarmed (col. 5, lines 5-13) and the security gateway is armed before connectivity with the security system server through the first network is restored (note the channel 36 is protected before sending video and alarm condition to the server, 38 of fig. 1).

5. Claims 57-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lemons (US 6,504,479) in view of Menard (US 6,667,688).

Re claims 57-61, Lemons teaches a security system (fig. 1) comprising: a security gateway located at a premises (12 of fig. 1), wherein the security gateway is operable to detect an alarm condition and to record video of at least a portion of the premises relating to the alarm condition, the video hereinafter referred to as an Alarm Video (16, 18, 20, 22, and 14 of fig. 1);

a security system server (38 of fig. 1) operatively coupled to the security gateway (12 of fig. 1) through a first network (36 of fig. 1), wherein the security gateway is configured to transfer to the security system server alarm information consisting of a first notification of the

alarm condition and the Alarm Video through the first network in substantially real time and wherein the security system server is remotely located relative to the security gateway (160 of fig. 3);

a monitoring center (48 of fig. 1) for monitoring video images, display alarms, display of contact data and information, wherein the video image and alarms received through network (36 or 50 of fig. 1), and any conventional channel communication networks include standard telephone service, ISDN, DSL, Internet, dedicated cable, local area network, wide area network, wireless, or any communications channel available to connect between the promise and server or other (col. 5, lines 15-22).

However, Lemons does not particularly teach the monitoring center operatively coupled to said security gateway through a second network, wherein the security gateway is configured to transfer to the monitoring center a second notification of the alarm condition without transferring the Alarm Video through the second network, wherein the monitoring center is remotely located relative to the security gateway and the security system server and wherein the monitoring center is further operably coupled to the security system server; and wherein the monitoring center is configured to transfer to the security system server a third notification of the alarm condition; wherein the monitoring center is operatively coupled to the security system server through a third network and wherein the monitoring center is configured to transfer to the security system server the third notification of the alarm condition through the third network; wherein the security system gateway is configured to transfer to the security gateway the alarm information through the first network substantially simultaneously with transferring to the monitoring station the second information of the alarm condition through the second network; wherein the monitoring

center is operatively coupled to the security system server through the first network and wherein the monitoring center is configured to transfer to the security system server the third notification of the alarm condition through the first network; wherein the security system gateway is configured to transfer to the security gateway the alarm information through the first network substantially simultaneously with transferring to the monitoring station the second notification of the alarm condition through the second network as specified in claims 57-61.

Menard teaches a monitoring center (30 and 40 of fig. 1, Note user communication device is considered as monitoring center) operatively coupled to said security gateway (10 of fig. 1) through a second network (Path A of fig. 1), wherein the security gateway (10 of fig. 1) is configured to transfer to the monitoring center a second notification of the alarm condition without transferring the Alarm Video through the second network (alarm transmission of fig. 1), wherein the monitoring center (30 and 40 of fig. 1) is remotely located relative to the security gateway (10 of fig. 1) and the security system server (20 of fig. 1) and wherein the monitoring center is further operably coupled to the security system server (30, 40, and 20 of fig. 1); and wherein the monitoring center is configured to transfer to the security system server a third notification of the alarm condition (Path D carries the same alarm transmission as Path A of fig. 1); wherein the monitoring center (30 and 40 of fig. 1) is operatively coupled to the security system server through a third network (Path D of fig. 1) and wherein the monitoring center (30 of fig. 1) is configured to transfer to the security system server the third notification of the alarm condition through the third network (Path C of fig. 1); wherein the security system gateway (10 of fig. 1) is configured to transfer to the security gateway of the alarm condition through the first network substantially simultaneously with transferring the monitoring station the second

notification of the alarm condition through the second network (Path A and Path B of fig. 1, Note simultaneous alarm transmission); wherein the monitoring center (30 and 40 of fig. 1) is operatively coupled to the security system server (Path D is the same Path A of fig. 1) through the first network and wherein the monitoring center is configured to transfer to the security system server the third notification of the alarm condition through the first network (Path A as Path D); wherein the security system gateway (10 of fig. 1) is configured to transfer to the security gateway (Alarm system) of the alarm condition through the first network substantially simultaneously with transferring the monitoring station the second notification of the alarm condition through the second network (Path A of fig. 1).

Therefore, taking the teachings of Lemons and Menard as a whole, it would have been obvious to one of ordinary skill in the art to modify the first and second networks (Path A and Path B of fig. 1) of Menard into the security system of Lemons for automatically transmitting notification of a detected alarm to the user. Doing so would save cost and simplify the security system.

6. Claims 20-24, 26-31, 47-52, and 57-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Saylor (US 6,400,265) in view of Kung et al. (US 6,826,173), and further in view of Menard et al. (US 6,667,688).

Re claim 20, Saylor teach a security system (fig. 1) comprising:

a security gateway located at premises (110, 120, 112, 122, 114, and 124 of fig. 1), wherein the security gateway is operable to detect an alarm condition and to record video of at

least a portion of the premises relating to the alarm condition, said video hereinafter referred to as an Alarm Video (120, 122, and 124 of fig. 1),

wherein the security gateway further comprises a network interface (100 of fig. 1, wherein the connections between the property (110 of fig. 1) and a security server (130 of fig. 1) throughout the network (100 of fig. 1)), and

wherein the network interface is configured to connect the security gateway to a cable head-end through a first network (Note the network (100 of fig. 1) between the property (110 of fig. 1) and the security server (130 of fig. 1);

a security system server (130 of fig. 1) configured to connect to the cable head-end through a second network (150 of fig. 1, Note alert notification is sent to the user and to the security system server through out the Internet), wherein the security gateway (110 of fig. 1) is configured to transfer to the security system server (130 of fig. 1) alarm information consisting of a first notification of the alarm condition (150 of fig. 1) and the Alarm Video in substantially real time through only the second network (150 of fig. 1, col. 4, lines 44-47, the alarm condition and alarm video would obviously be transmitted through the second network, 150 of fig. 1);

wherein the security gateway (110 of fig. 1) is operatively coupled to the security system server (130 of fig. 1) through a third network (152 of fig. 1; Note alert notification is transmitted to the user and to the security system server through POTS (cable)), the security gateway (110 of fig. 1) being further configured to transfer to the security system server (130 of fig. 1) a second notification of the alarm condition through the third network (152 of fig. 1); and

wherein the security gateway (110 of fig. 1) is configured to transfer the alarm information to the security system server through the second network substantially

simultaneously *(Note a system and method for monitoring a security system by using video images where a wireless communication system may be used to automatically inform an owner and other authorized entities in a manner predetermined by the user when alarm situations and/or alarm worthy situations occur, this suggests the security gateway simultaneously transmits the alarm notification to the second and third networks*) with transferring the second notification of the alarm condition to the security system server (130 of fig. 1) through the second and third networks (150 and 152 of fig. 1); wherein the security system server is configured to receive the alarm video (see fig. 10, wherein the video image is transmitted from the camera to the server).

It is noted that Saylor suggests that phone, POTS, cable, DSL, and other combinations may be implemented (col. 6, lines 21-33), so this is evidence to one skill in the art to modify any conventional and suitable connection between the security server and the security gateway of Saylor.

However, Saylor does particularly teach the first network is a hybrid-fiber- coaxial network as claimed.

Kung teaches a security gateway (102 of fig. 1) connects to a cable head-end (115 of fig. 1) through a first network (112 of fig. 1) by a hybrid-fiber-coaxial network (col.5, line 44 through col. 6, line 9).

Therefore, taking the teachings of Saylor and Kung as a whole, it would have been obvious to one of ordinary skill in the art to incorporate the cable head-end (115 of fig. 1) through the first network (112 of fig. 1) by the hybrid-fiber-coaxial network (col.5, line 44 through col. 6, line 9) of Kung into the networks of Saylor for enhancing the functionality of

components in the broadband network. Doing so would allow the system to provide ease of maintenance, control, and re-configuration as well as a reduction in cost due to shared functionality.

It is noted that Saylor does not particularly wherein the security system server is configured to receive the first notification of the alarm condition through the second network and to receive the second notification of the alarm condition through the third network as claimed.

Tsumpes teaches simultaneously transferring the alarm to the security server (13 of fig. 1) of the alarm through the second network (19 of fig. 1) and the third network (20 of fig. 1), and wherein the security system server (13 of fig. 1) is configured to receive a notification of the alarm condition through the second network (19 of fig. 1) and to receive another notification of the alarm condition through the third network (20 of fig. 1; *note* one of the major benefits of the present pre-programmed and automated *parallel* and *redundant* contact and notification system and method is that it provides expeditious and efficient handling of time sensitive events and significantly reduces response time in emergency situations (col.8, lines 18-23). The disclosure above fairly suggests the communications networks (19 and 20 of fig. 1)are in parallel and redundant (note the communications networks are in parallel that would obviously transmit the notifications simultaneously, and the communications networks are in redundant that would obviously transmit the notification via the first communication network or the second communication network as back-up network, or redundantly transmit the notification through fist and second networks substantially at the same time).

Therefore, taking the teachings of Saylor, Kung, and Tsumpes as a whole, it would have been obvious to one of ordinary skill in the art to modify the teachings of Tsumpes, the

automated parallel and redundant contact to a user notification one or more alarms, into the security system of Saylor and Kung for one of the major benefits of the automated parallel and redundant contact and notification system and method is that it provides expeditious and efficient handling of time sensitive events and significantly reduces response time in emergency situations.

Re claim 21, Saylor teaches wherein the second network is a dedicated bandwidth network (Internet 150 of fig. 1).

Re claim 22, Saylor further teaches wherein the second network comprises a frame relay network (230 of fig. 1).

Re claim 23, Saylor further teaches wherein the second network comprises an ATM network (other methods are considered as an ATM network, col. 4, lines 46-47).

Re claim 24, Saylor further teaches wherein the second network comprises a managed IP connection having quality of service (TCP/IP connection of fig. 2).

Re claim 26, Saylor further teaches wherein the third network comprises a public switched telephone network (POTS 152 of fig. 1).

Re claim 27, Saylor further teaches wherein the third network comprises a fixed wireless network (fig. 2).

Re claim 28, Saylor further teaches wherein the third network comprises a mobile communications network (col. 4, line 46).

Re claim 29, Saylor further teaches wherein the security gateway is further operable to record audio from at least a portion of the premises relating to the alarm condition, said audio referred hereinafter as Alarm Audio, and wherein the security gateway is further configured to

transmit said Alarm Audio to the security system server through the second network in substantially real time (col. 8, lines 50-65).

Re claim 30, Saylor further teaches wherein the security system server (130 of fig. 1) is configured to provide notification of the alarm condition to a public safety agency (160f-160N of fig. 1; see also 164 of fig. 1).

Re claim 31, Saylor further teaches wherein the security system server is further configured to provide the Alarm Video to the public safety agency (video 110 of fig. 1).

Re claim 47, Saylor further teaches wherein the security gateway is further configured to detect if connectivity with the security system server through the first network is lost and transfer to the security system server through the second network of the loss of connectivity through the first network (col. 6, lines 50-55).

Re claim 48, Saylor further teaches wherein the security gateway is further configured to transfer to the security system server in the event that connectivity with the security system server through the first network is lost while the security gateway is disarmed and the security gateway is armed before connectivity with the security system server through the first network is restored (col. 6, lines 21-34).

Re claim 49, Saylor further teaches wherein the security gateway is further configured to detect if connectivity with the security system server through the first network is lost and transfer to the security system server through the second network of the loss of connectivity through the first network (col. 6, lines 21-34).

Re claim 50, Saylor further teaches wherein the security gateway is further configured to detect if connectivity with the security system server through the first network is lost and

transfer to the security system server through the second network of the loss of connectivity through the first network (col. 6, lines 21-34).

Re claim 51, Saylor further teaches wherein the security gateway is further configured to transfer to the security system server in the event that connectivity with the security system server through the first network is lost while the security gateway is disarmed and the security gateway is armed before connectivity with the security system server through the first network is restored (col. 6, lines 21-55).

Re claim 52, Saylor further teaches wherein the security gateway is further configured to detect if connectivity with the security system server through the first network is lost and transfer to the security system server through the second network of the loss of connectivity through the first network (col. 6, lines 21-55).

Re claim 57, Saylor further teaches a security system (fig. 1) comprising: a security gateway located at a premises (110, 120, 112, 122, 114, 124 of fig. 1), wherein the security gateway is operable to detect an alarm condition and to record video of at least a portion of the premises relating to the alarm condition, the video hereinafter referred to as an Alarm Video;

a security system server (130 of fig. 1) operatively coupled to the security gateway through a first network, wherein the security gateway is configured to transfer to the security system server alarm information consisting of a first notification of the alarm condition and the Alarm Video through the first network in substantially real time and wherein the security system server is remotely located relative to the security gateway (Note the connections between the security server and the property would obviously be considered as a first network, see 110, 130 of fig. 1));

a monitoring center (160 of fig. 1) operatively coupled to said security gateway through a second network (150 of fig. 1), wherein the security gateway is configured to transfer to the monitoring center a second notification of the alarm condition through the second network, wherein the monitoring center (160 of fig. 1) is remotely located relative to the security gateway and the security system server and wherein the monitoring center is further operably coupled to the security system server (130 of fig. 1); and wherein the monitoring center is configured to transfer to the security system server a third notification of the alarm condition (160 of fig. 1).

Re claim 58, Saylor further discloses wherein the monitoring center is operatively coupled to the security system server (130 of fig. 1) through a third network (152 of fig. 1) and wherein the monitoring center is configured to transfer to the security system server the third notification of the alarm condition through the third network.

Re claim 59, Saylor further teaches wherein the security system gateway is configured to transfer to the security gateway the alarm information through the first network substantially simultaneously with transferring to the monitoring station the second notification of the alarm condition through the second network (col. 1, lines 5-13).

Re claim 60, Saylor further teaches wherein the monitoring center (160 of fig. 1) is operatively coupled to the security system server (130 of fig. 1) through the first network (Internet) and wherein the monitoring center is configured to transfer to the security system server third notification of the alarm condition through the first network.

Re claim 61, Saylor further teaches wherein the security system gateway (110 and 120 of fig. 1) is configured to transfer to the security gateway of the alarm information through the first

network substantially simultaneously with transferring to the monitoring station the second notification of the alarm condition through the second network (col. 1, lines 5-13).

Response to Arguments

1. Applicant's arguments filed 12/02/2009 have been fully considered but they are not persuasive.

The applicant argues that none of the cited references Tsumpes, Lemons, Menard, Kung and/or Saylor, either alone or in combination, teaches or suggests each and every element of independent claims 1 and 20 as hereby amended at least because none of these references teaches transferring Alarm Video associated with an alarm condition through only one of two networks substantially simultaneously with transferring alarm notifications of the alarm condition through both of the two networks.

The examiner respectively disagrees with the applicant. It is submitted that Tsumpes teaches transferring Alarm Video associated with an alarm condition (the cellular communications network, col. 5, lines 19-23) through only one of two networks substantially simultaneously with transferring alarm notifications of the alarm condition (DDP includes alarm notifications, col. 3, lines 54-62) through both of the two networks (e.g. the cellular communications network and a radio frequency RF, col. 5, lines 19-23, e.g. 19 and 20 of fig. 1).

The Applicants submit that none of the cited references Tsumpes, Lemons, Menard, Kung and/or Saylor, either alone or in combination, teaches or suggests each and every element of independent claim 57 as hereby amended at least because none of these references discloses a security gateway transferring both an Alarm Video and a first notification of an alarm condition

to a security system server through a first network, the security gateway transferring a second notification of the alarm condition without the Alarm Video to a monitoring center through a second network, and the monitoring center transferring a third notification of the alarm condition to the security system server.

The examiner respectively disagrees with the applicant. It is submitted that Menard teaches a security gateway (10 of fig. 1) transferring both an Alarm Video and a first notification of an alarm condition to a security system server through a first network (Path B of fig. 1), the security gateway transferring a second notification of the alarm condition without the Alarm Video to a monitoring center (40 of fig. 1) through a second network (Path B of fig. 1), and the monitoring center (40 of fig. 1) transferring a third notification of the alarm condition to the security system server (Path C and 20 of fig. 1).

(10) Response to Argument

A. 103 (a) Obviousness Rejection of Tsumpes- The cited prior art teach obvious every element of claimed invention.

Tsumpes teaches a security system (fig. 1) comprising: a security gateway *(12 of fig. 1, the controller is considered as a security gateway)* located at a premises *(11of fig. 1, sensors are obviously alarm and video systems)*, wherein the security gateway (12 of fig. 1) is operable to detect an alarm condition *(col. 6, lines 32-37)* and to record video of at least a portion of the premises relating to the alarm condition, said video hereinafter referred to as an Alarm Video *(Alarm inputs, 11 of fig. 1, wherein alarm inputs 11 are video that would obviously be considered as alarm video; col. 8, lines 45-50, note the digital data packet DDP and wireless or*

Internet communication network also enables the present system to provide video and/or audio transmissions from the monitored device or premises to the central monitoring station due to the bandwidth capabilities of most digital data packet networks); a security system server (13 of fig. 1) operatively coupled to the security gateway through a first network (19 of fig. 1) and a second network (20 of fig. 1); wherein the security gateway*(12of fig. 1, the controller is considered as a security gateway)* is to transfer ***alarm information consisting of*** the Alarm Video (e.g. 11 of fig. 1, note *wherein alarm inputs 11 are video)* the and ***a first notification of the alarm condition (e.g. DDP includes notification of the alarm condition)*** to the security system server in substantially real time through only the first network *(col. 4, line 64-col. 5, line 33, transmission of notification alarms between the security gateway and the security system server, 12 and 13 of fig. 1; col. 8, lines 45-50, note the digital data packet DDP and wireless or Internet communication network also enables the present system to provide video and/or audio transmissions from the monitored device or premises to the central monitoring station due to the bandwidth capabilities of most digital data packet networks, therefore one skill in the art would used this suggestion to design the system for transmitting the video through only the first network, 19 of fig. 1);* wherein the security gateway (12 of fig. 1) is further configured to ***transfer to*** the security system server ***a second notification*** of the alarm condition (Another input 11 has a second notification of the alarm condition) through the ***second*** network (19 and 20 of fig. 1, col. 5, lines 19-23, note DDP is transmitted via the wireless transceiver and radio frequency RF transceiver), and wherein the security system server thereby receives the Alarm Video, the first notification of the alarm condition, and the second notification of the alarm condition from the security gateway (the central monitoring station security system server

receives one or more alarms from the premises, col. 1, lines 15-25, and Digital Data Packet that include the Alarm Video, col. 8, lines 45-50); transmitting the second notification of the alarm condition through second network (20 of fig. 1) substantially simultaneously with transferring the alarm information to the security server through the first network (col.8, lines 18-23).

1. Claims 1, 3-15, and 17-19- Tsumpes does teach substantially simultaneous transfer of two different alarm signals from security gateway to security system sever through a first and second networks.

a. The cited art does teach substantially simultaneous transfer alarm:

The appellant argues that Tsumpes does not teach the security gateway is further configured transfer to the security system server a second notification of the alarm condition through the second network substantially simultaneously with transferring the alarm notification to the security system server through the first network.

The examiner respectfully disagrees with the applicant. It is submitted that Tsumpes teaches the security gateway (12 of fig. 1) is further configured transfer to the security system server (13 of fig. 1) a second notification of the alarm condition (11 of fig. 1, note the sensors 11 are monitoring simultaneously a plurality of different events, and the second notification of the alarm condition is one of the plurality event) through the second network (col. 5, lines 19-23) substantially simultaneously (20 of fig. 1) with transferring the alarm notification (11 of fig.1, the first monitored alarm condition is sent by the controller 12 through the fist network, 19 of fig. 1) to the security system server (13 of fig. 1) through the first network (19 of fig. 1, note the digital data packet DDP of the first sensor, 11 of fig. 1, is transmitted through the first network,

19 of fig. 1; and the digital data packet DDP of the second sensor, 11 of fig. 1, is transmitted through the second network, 20 of fig. 1).

Note Tsumpes further teaches the system enables automated simultaneous contact of one or more persons over a plurality of telephonic and electronic communication channels and provides parallel event-specific notification via voice, pager, voice mail, fax and email to the recipient(s) that are identified by electronic or speech recognized entry of a PIN and then provides them with a detailed message including the date and time of a specific event which has occurred or failed to occur with respect to a monitored sensor (col. 4, lines 5-11).

The above disclosure suggests one skill in the art would modify the suggested teachings of Tsumpes (col. 4, lines 5-13) into the system (fig. 1) to enable automated simultaneous transfer one or more alarm conditions from the sensors (11 of fig. 1) over a plurality of telephonic and electronic communication channels (14, 17, 19, and 20 of fig. 1).

Note Tsumpes discloses one of the major benefits of the present pre-programmed and automated ***parallel*** and ***redundant*** contact and notification system and method is that it provides expeditious and efficient handling of time sensitive events and significantly reduces response time in emergency situations (col. 8, lines 18-23). The communications networks are in parallel that would obviously transmit the notifications simultaneously, and the communications networks are in redundant that would obviously transmit the notification via the first communication network or the second communication network as back-up network, or redundantly transmit the notification through fist and second networks substantially at the same time.

The above disclosure fairly suggests the communications networks (19 and 20 of fig. 1) are in parallel for substantially simultaneously transmitting notifications (col. 1, lines 1, lines 15-25, col. 4, lines 5-13) of the alarm conditions with transferring the alarm information to the central monitoring system (13 o fig. 1) for many benefits including reduction of false alarms and false dispatches.

b. The cited prior art does teach transfer of two different alarm signals over two networks.

The appellant argues that Tsumpes does not teach (1) "the security gateway is configured to transfer alarm information consisting of Alarm Video and a first notification of the alarm condition to the security system server in substantially real time through only the first network," and (2) "the security gateway is further configured to transfer to the security system server a second notification of the alarm condition through the second network."

The examiner respectfully disagrees with the applicant. It is submitted that Tsumpes teaches the security gateway (12 of fig. 1) is further configured transfer to the security system server (13 of fig. 1) a second notification of the alarm condition (11 of fig. 1, note the sensors 11 are monitoring simultaneously a plurality of different events, and the second notification of the alarm condition is one of the plurality event) through the second network (col. 5, lines 19-23) substantially simultaneously (20 of fig. 1) with transferring the alarm notification (11 of fig.1, the first monitored alarm condition is sent by the controller 12 through the fist network, 19 of fig. 1) to the security system server (13 of fig. 1) through the first network (19 of fig. 1, note the digital data packet DDP of the first sensor, 11 of fig. 1, is transmitted through the first network,

19 of fig. 1; and the digital data packet DDP of the second sensor, 11 of fig. 1, is transmitted through the second network, 20 of fig. 1).

Note Tsumpes further teaches the system enables automated simultaneous contact of one or more persons over a plurality of telephonic and electronic communication channels and provides parallel event-specific notification via voice, pager, voice mail, fax and email to the recipient(s) that are identified by electronic or speech recognized entry of a PIN and then provides them with a detailed message including the date and time of a specific event which has occurred or failed to occur with respect to a monitored sensor (col. 4, lines 5-11).

The above disclosure suggests one skill in the art would modify the suggested teachings of Tsumpes (col. 4, lines 5-13) into the system (fig. 1) to enable automated simultaneous transfer one or more alarm conditions from the sensors (11 of fig. 1) over a plurality of telephonic and electronic communication channels (14, 17, 19, and 20 of fig. 1).

Note Tsumpes discloses one of the major benefits of the present pre-programmed and automated ***parallel*** and ***redundant*** contact and notification system and method is that it provides expeditious and efficient handling of time sensitive events and significantly reduces response time in emergency situations (col. 8, lines 18-23). The communications networks are in parallel that would obviously transmit the notifications simultaneously, and the communications networks are in redundant that would obviously transmit the notification via the first communication network or the second communication network as back-up network, or redundantly transmit the notification through fist and second networks substantially at the same time.

The above disclosure fairly suggests the communications networks (19 and 20 of fig. 1) are in parallel for substantially simultaneously transmitting notifications (col. 1, lines 1, lines 15-25, col. 4, lines 5-13) of the alarm conditions with transferring the alarm information to the central monitoring system (13 o fig. 1) for many benefits including reduction of false alarms and false dispatches.

2. Claim 16- Tsumpes teaches substantially simultaneous transfer of alarm video and first notification through the first network and transfer of alarm audio and second notification through the second network.

The appellant argues that Tsumpes does not teach substantially simultaneous transfer of alarm video and first notification through the first network and transfer of alarm audio and second notification through the second network.

The examiner strongly disagrees with the appellant. It is submitted that Tsumpes teaches the security gateway (12 of fig. 1) substantially simultaneous transfer of alarm video and first notification (11 of fig. 1, note the sensors 11 are monitoring simultaneously a plurality of different events, and the video alarm and first notification is one of the plurality event) through the first network (19 of fig. 1) and transfer of alarm audio and second notification through the second network (11 of fig. 1, note the sensors 11 are monitoring simultaneously a plurality of different events, and the audio and second notification of the alarm condition is one of the plurality event, note sensor 11 is audio and video data, col. 6, lines 32-65 and col. 8, lines 45-50) through the second network (col. 5, lines 19-23; note the digital data packet DDP of the first sensor, 11 of fig. 1, is transmitted through the first network, 19 of fig. 1; and the digital data

packet DDP of the second sensor, 11 of fig. 1, is transmitted through the second network, 20 of fig. 1).

Note Tsumpes further teaches the system enables automated simultaneous contact of one or more persons over a plurality of telephonic and electronic communication channels and provides parallel event-specific notification via voice, pager, voice mail, fax and email to the recipient(s) that are identified by electronic or speech recognized entry of a PIN and then provides them with a detailed message including the date and time of a specific event which has occurred or failed to occur with respect to a monitored sensor (col. 4, lines 5-11).

The above disclosure suggests one skill in the art would modify the suggested teachings of Tsumpes (col. 4, lines 5-13) into the system (fig. 1) to enable automated simultaneous transfer one or more alarm conditions from the sensors (11 of fig. 1) over a plurality of telephonic and electronic communication channels (14, 17, 19, and 20 of fig. 1).

Note Tsumpes discloses one of the major benefits of the present pre-programmed and automated ***parallel*** and ***redundant*** contact and notification system and method is that it provides expeditious and efficient handling of time sensitive events and significantly reduces response time in emergency situations (col. 8, lines 18-23). The communications networks are in parallel that would obviously transmit the notifications simultaneously, and the communications networks are in redundant that would obviously transmit the notification via the first communication network or the second communication network as back-up network, or redundantly transmit the notification through fist and second networks substantially at the same time.

The above disclosure fairly suggests the communications networks (19 and 20 of fig. 1) are in parallel for substantially simultaneously transmitting video, audio, and notifications (col. 1, lines 1, lines 15-25, col. 4, lines 5-13) of the alarm conditions to the central monitoring system (13 o fig. 1) for many benefits including reduction of false alarms and false dispatches.

B. 103 (a) Obviousness Rejection of Tsumpes in vie of Lemons-The cited prior art discloses notifying the security server of loss of connectivity.

The appellant argues that Lemons does not teach notifying the security system server of loss of connectivity.

The examiner strongly disagrees with the applicant. It is submitted that Lemons teaches wherein the security gateway (12 of fig. 1) is further configured to detect if connectivity with the security system server through the first network (36 of fig. 1, note the backup communications channel, 50 of fig. 1, is connected when the first network, 36 of fig. 1, is interrupted) is lost and transfer to the security system server by sending a notification signal through the second network of the loss of connectivity through the first network (Note in case the channel 36 is broken, interrupted, or otherwise impaired, the controller 200 is connected to the monitoring center 38 via the CTE252 and the communications channel 50, col. 9, lines 51-61, wherein the controller 200 is capable of responding to commands from one of the workstation 38 of fig. 1, e.g. lost of the connectivity); wherein the security gateway (12 of fig. 1) is further configured to transfer to the security system server (38 of fig. 1) in the event that connectivity with the security system server through the first network is lost (e.g. 36 of fig. 1, the channel 36 is interrupted, col. 9, lines 51-61) while the security gateway is disarmed (col. 5, lines 5-13) and the security gateway is

armed before connectivity with the security system server through the first network is restored (note the channel 36 is protected before sending video and alarm condition to the server, 38 of fig. 1).

C. 103(a) Obviousness Rejection of Lemons in view of Tsumpes and Kung.

Teaching, suggestion, or motivation

The appellants traverse the rejections because there is no teaching, suggestion, or motivation cited.

In response to appellant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992).

Hindsight reconstruction

The appellant argued that the rejections based on hindsight reconstruction of claimed invention.

In response to appellant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the

time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

Established a prima facie showing of obviousness

The office has not established a prima facie case of obviousness and the rejections are not support by concrete evidence of record.

In response to appellant's argument, the examiner would like point out the following basic principle of a proper prior art analysis within 35 U.S.C. 103 (a).

Not only the specific teachings of a reference but also reasonable inferences which the artisan would have logically drawn therefrom may be properly evaluated in formulating a rejection. In re Preda, 401 F.2d 825, 159 USPQ 342 (CCPA 1968) and In re Shepard, 319 F.2d 194, 138 USPQ 148 (CCPA 1963). Skill in the art is presumed. In re Sovish, 769 F.2d 738, 226 USPQ 771 (Fed. Cir. 1985). Furthermore, artisans must be presumed to know something about the art apart from what the references disclose. In re Jacoby, 309 F.2d 513, 135 USPQ 317 (CCPA 1962). The obviousness may be made from common knowledge and common sense of a person of ordinary skill in the art without any specific hint or suggestion in a particular reference. In re Bozek, 416 F.2d 1385, 163 USPQ 545 (CCPA 1969)). Every reference relies to some extent on knowledge of persons skilled in the art to complement that which is disclosed therein. In re Bode, 550 F.2d 656, 193 USPQ 12 (CCPA 1977).

1. Claims 20-23 and 26-31- The cited prior art teach the substantially simultaneous transfer of alarm from security gateway to security system server through a fist and a second network or transmission of two different signals over the two networks.

a. The cited prior art does teach substantially simultaneous transfer of alarm

b. The cited prior art does not teach two different signal

The appellant argues that Lemons and Tsumpes do not teach **substantially simultaneous transfer of alarm or two different signals.**

The examiner respectfully disagrees with the applicant. It is submitted that Lemons teaches a security system (fig. 1) comprising a security gateway (12 of fig. 1) located at a premises (12a and 12b of fig. 8), wherein the security gateway (12 of fig. 1) is operable to detect an alarm condition and to record video of at least a portion of the premises relating to the alarm condition to form an alarm video (16, 18, 20, 22 of fig. 1; see fig. 3), wherein the security gateway (12 of fig. 1) further comprises a network interface (14 of fig. 1, Note the connections between the components (24, 26, 28, 30, 34, 56 of fig. 1), and wherein the network interface is configured to connect the security gateway a head-end through out a first network (col. 6, line 62-col. 7, lines 50, Note the connections between components are considered as the first network; a network is a fabric or structure of cords or wires that cross at regular intervals and are knotted or secured at the crossings, a system of lines or channels resembling a network, an interconnected or interrelated chain, group, or system, or a system of computers, peripherals, terminals, and databases connected by communications lines); a security system server (38 of fig. 1) configured to connect to the interface (34 of fig. 1) through a second network (36 of fig. 1), wherein the security gateway (12 and 14 of fig. 1) is configured to **transfer to** the security system server **alarm information consisting of a first notification** of the alarm condition and the Alarm Video to the security system server in substantially real time (col. 7, lines25-50) only through the second network (36 of fig.1, the alarm condition and alarm video is transmitted to

the server using the network as the second network); wherein the security gateway (12, 14 of fig. 1) is operatively coupled to the security system server (38 of fig. 1) through a third network (50 of fig. 1) for redundant transmitting the alarm condition, the security gateway being further configured to **transfer to** the security system server of the alarm condition through the third network (col. 4, line 66 through col. 5, lines 14); wherein the security gateway is configured to transfer the alarm information to the security system server through the second network (36 of fig.1, the alarm condition and alarm video is transmitted to the server using the network as the second network).

Lemons suggests that any communications channel available (36 and 50 of fig. 1) such as a hybrid-fiber coaxial network; a fiber-optic network, an ATM network, and a high-speed mobile communications network, that connects between the gateway (12 of fig. 1) is used in the security system, so this is evidence to one skilled in the art to modify any conventional network into the security system of Lemons.

Tsumpes teaches the security gateway (12 of fig. 1) substantially simultaneous transfer of alarm video and first notification (11 of fig. 1, note the sensors 11 are monitoring simultaneously a plurality of different events, and the video alarm and first notification is one of the plurality event) through the first network (19 of fig. 1) and transfer of alarm audio and second notification through the second network (11 of fig. 1, note the sensors 11 are monitoring simultaneously a plurality of different events, and the audio and second notification of the alarm condition is one of the plurality event, note sensor 11 is audio and video data, col. 6, lines 32-65 and col. 8, lines 45-50) through the second network (col. 5, lines 19-23; note the digital data packet DDP of the first sensor, 11 of fig. 1, is transmitted through the first network, 19 of fig. 1; and the digital data

packet DDP of the second sensor is considered as a second signal, 11 of fig. 1, and transmitted through the second network, 20 of fig. 1).

Note Tsumpes further teaches the system enables automated simultaneous contact of one or more persons over a plurality of telephonic and electronic communication channels and provides parallel event-specific notification via voice, pager, voice mail, fax and email to the recipient(s) that are identified by electronic or speech recognized entry of a PIN and then provides them with a detailed message including the date and time of a specific event which has occurred or failed to occur with respect to a monitored sensor (col. 4, lines 5-11).

The above disclosure suggests one skill in the art would modify the suggested teachings of Tsumpes (col. 4, lines 5-13) into the system (fig. 1) to enable automated simultaneous transfer one or more alarm conditions from the sensors (11 of fig. 1) over a plurality of telephonic and electronic communication channels (14, 17, 19, and 20 of fig. 1).

Note Tsumpes discloses one of the major benefits of the present pre-programmed and automated ***parallel*** and ***redundant*** contact and notification system and method is that it provides expeditious and efficient handling of time sensitive events and significantly reduces response time in emergency situations (col. 8, lines 18-23). The communications networks are in parallel that would obviously transmit the notifications simultaneously, and the communications networks are in redundant that would obviously transmit the notification via the first communication network or the second communication network as back-up network, or redundantly transmit the notification through fist and second networks substantially at the same time.

The above disclosure fairly suggests the communications networks (19 and 20 of fig. 1) are in parallel for substantially simultaneously transmitting video, audio, and notifications (col. 1, lines 1, lines 15-25, col. 4, lines 5-13) of the alarm conditions to the central monitoring system (13 o fig. 1) for many benefits including reduction of false alarms and false dispatches.

Taking the teachings of Lemons and Tsumpes as a whole, it would have been obvious to one of ordinary skill in the art to modify the teachings of Tsumpes, the automated parallel and redundant contact to a user notification one or more alarms, into the security system of Lemons for one of the major benefits of the automated parallel and redundant contact and notification system and method is that it provides expeditious and efficient handling of time sensitive events and significantly reduces response time in emergency situations.

2. Claims 50-52-The cited prior at disclose notification the security system server of loss of connectivity.

The appellant argues that Lemons in view of Tsumpes and Kung does not teach notifying the security system server of loss of connectivity.

The examiner respectfully disagrees with the appellant. It is submitted that Lemons teaches wherein the security gateway (12 of fig. 1) is further configured to detect if connectivity with the security system server through the first network (36 of fig. 1, note the backup communications channel, 50 of fig. 1, is connected when the first network, 36 of fig. 1, is interrupted) is lost and transfer to the security system server by sending a notification signal through the second network of the loss of connectivity through the first network (Note in case the channel 36 is broken, interrupted, or otherwise impaired, the controller 200 is connected to the monitoring center 38 via the CTE252 and the communications channel 50, col. 9, lines 51-

61, wherein the controller 200 is capable of responding to commands from one of the workstation 38 of fig. 1, e.g. lost of the connectivity); wherein the security gateway (12 of fig. 1) is further configured to transfer to the security system server (38 of fig. 1) in the event that connectivity with the security system server through the first network is lost (e.g. 36 of fig. 1, the channel 36 is interrupted, col. 9, lines 51-61) while the security gateway is disarmed (col. 5, lines 5-13) and the security gateway is armed before connectivity with the security system server through the first network is restored (note the channel 36 is protected before sending video and alarm condition to the server, 38 of fig. 1).

D. 103(a) Obviousness Rejection - Lemons in view of Menard.

The appellant argues that (1) a security gateway "configured to transfer to the security system server alarm information consisting of a first notification of the alarm condition and the Alarm Video through the first network in substantially real time," (2) with the security gateway also "configured to transfer to the monitoring center a second notification of the alarm condition without transferring the Alarm Video through the second network," and (3) "the monitoring center configured to transfer to the security system server a third notification of the alarm condition."

The examiner respectfully disagrees with the applicant. It is submitted that Lemons teaches a security system (fig. 1) comprising: a security gateway located at a premises (12 of fig. 1), wherein the security gateway is operable to detect an alarm condition and to record video of at least a portion of the premises relating to the alarm condition, the video hereinafter referred to as an Alarm Video (16, 18, 20, 22, and 14 of fig. 1); a security system server (38 of fig. 1) operatively coupled to the security gateway (12 of fig. 1) through a first network (36 of fig. 1),

wherein the security gateway is configured to transfer to the security system server alarm information consisting of a first notification of the alarm condition and the Alarm Video through the first network in substantially real time and wherein the security system server is remotely located relative to the security gateway (160 of fig. 3); a monitoring center (48 of fig. 1) for monitoring video images, display alarms, display of contact data and information, wherein the video image and alarms received through network (36 or 50 of fig. 1), and any conventional channel communication networks include standard telephone service, ISDN, DSL, Internet, dedicated cable, local area network, wide area network, wireless, or any communications channel available to connect between the promise and server or other (col. 5, lines 15-22).

Menard teaches a monitoring center (30 and 40 of fig. 1, Note user communication device is considered as monitoring center) operatively coupled to said security gateway (10 of fig. 1) through a second network (Path A of fig. 1), wherein the security gateway (10 of fig. 1) is configured to transfer to the monitoring center a second notification of the alarm condition without transferring the Alarm Video through the second network (alarm transmission of fig. 1), wherein the monitoring center (30 and 40 of fig. 1) is remotely located relative to the security gateway (10 of fig. 1) and the security system server (20 of fig. 1) and wherein the monitoring center is further operably coupled to the security system server (30, 40, and 20 of fig. 1); and wherein the monitoring center is configured to transfer to the security system server a third notification of the alarm condition (Path D carries the same alarm transmission as Path A of fig. 1); wherein the monitoring center (30 and 40 of fig. 1) is operatively coupled to the security system server through a third network (Path D of fig. 1) and wherein the monitoring center (30 of fig. 1) is configured to transfer to the security system server the third notification of the alarm

condition through the third network (Path C of fig. 1); wherein the security system gateway (10 of fig. 1) is configured to transfer to the security gateway of the alarm condition through the first network substantially simultaneously with transferring the monitoring station the second notification of the alarm condition through the second network (Path A and Path B of fig. 1, Note simultaneous alarm transmission); wherein the monitoring center (30 and 40 of fig. 1) is operatively coupled to the security system server (Path D is the same Path A of fig. 1) through the first network and wherein the monitoring center is configured to transfer to the security system server the third notification of the alarm condition through the first network (Path A as Path D); wherein the security system gateway (10 of fig. 1) is configured to transfer to the security gateway (Alarm system) of the alarm condition through the first network substantially simultaneously with transferring the monitoring station the second notification of the alarm condition through the second network (Path A of fig. 1).

Menard further teaches a security gateway (10 of fig. 1) transferring both an Alarm Video and a first notification of an alarm condition to a security system server through a first network (Path B of fig. 1), the security gateway transferring a second notification of the alarm condition without the Alarm Video to a monitoring center (40 of fig. 1) through a second network (Path B of fig. 1), and the monitoring center (40 of fig. 1) transferring a third notification of the alarm condition to the security system server (Path C and 20 of fig. 1).

Taking the teachings of Lemons and Menard as a whole, it would have been obvious to one of ordinary skill in the art to modify the first and second networks (Path A and Path B of fig. 1) of Menard into the security system of Lemons for automatically transmitting notification of a detected alarm to the user to reduce cost and simplify the security system.

E. 103(a) Obvious Rejection of Saylor in view of Tsumpes and Kung.

1. Claims 20-24 and 26-31-The cited prior art teaches substantially simultaneous transfer of alarm through the first network and the second network or the required network connections.

a. The cited prior art does not disclose substantially simultaneous transfer alarm.

The appellant argues that Saylor does not teach "the security gateway is configured to transfer the alarm information to the security system server through the second network substantially simultaneously with transferring the second alarm notification to the security system server through the third network."

The examiner respectfully disagrees with the applicant. It is submitted that Saylor teach a security system (fig. 1) comprising: a security gateway located at premises (110, 120, 112, 122, 114, and 124 of fig. 1), wherein the security gateway is operable to detect an alarm condition and to record video of at least a portion of the premises relating to the alarm condition, said video hereinafter referred to as an Alarm Video (120, 122, and 124 of fig. 1), wherein the security gateway further comprises a network interface (100 of fig. 1, wherein the connections between the property (110 of fig. 1) and a security server (130 of fig. 1) throughout the network (100 of fig. 1)), and wherein the network interface is configured to connect the security gateway to a cable head-end through a first network (Note the network (100 of fig. 1) between the property (110 of fig. 1) and the security server (130 of fig. 1); a security system server (130 of fig. 1) configured to connect to the cable head-end through a second network (150 of fig. 1, Note alert notification is sent to the user and to the security system server through out the Internet), wherein the security gateway (110 of fig. 1) is configured to transfer to the security system server (130 of

fig. 1) alarm information consisting of a first notification of the alarm condition (150 of fig. 1) and the Alarm Video in substantially real time through only the second network (150 of fig. 1, col. 4, lines 44-47, the alarm condition and alarm video would obviously be transmitted through the second network, 150 of fig. 1); wherein the security gateway (110 of fig. 1) is operatively coupled to the security system server (130 of fig. 1) through a third network (152 of fig. 1; Note alert notification is transmitted to the user and to the security system server through POTS (cable)), the security gateway (110 of fig. 1) being further configured to transfer to the security system server (130 of fig. 1) a second notification of the alarm condition through the third network (152 of fig. 1); and wherein the security gateway (110 of fig. 1) is configured to transfer the alarm information to the security system server through the second network substantially simultaneously *(Note a system and method for monitoring a security system by using video images where a wireless communication system may be used to automatically inform an owner and other authorized entities in a manner predetermined by the user when alarm situations and/or alarm worthy situations occur, this suggests the security gateway simultaneously transmits the alarm notification to the second and third networks*) with transferring the second notification of the alarm condition to the security system server (130 of fig. 1) through the second and third networks (150 and 152 of fig. 1); wherein the security system server is configured to receive the alarm video (see fig. 10, wherein the video image is transmitted from the camera to the server).

Tsumpes teaches transferring Alarm Video associated with an alarm condition (the cellular communications network, col. 5, lines 19-23) through only one of two networks substantially simultaneously with transferring alarm notifications of the alarm condition (DDP

includes alarm notifications, col. 3, lines 54-62) through both of the two networks (e.g. the cellular communications network and a radio frequency RF, col. 5, lines 19-23, e.g. 19 and 20 of fig. 1).

b. The cited prior art teach claimed network connections.

The appellant argues that Saylor does not teach the claimed network connections.

The examiner respectfully disagrees with the applicant. It is submitted Saylor suggests that phone, POTS, cable, DSL, and other combinations may be implemented (col. 6, lines 21-33), so this is evidence to one skill in the art to modify any conventional and suitable connection between the security server and the security gateway of Saylor.

Kung teaches a security gateway (102 of fig. 1) connects to a cable head-end (115 of fig. 1) through a first network (112 of fig. 1) by a hybrid-fiber-coaxial network (col.5, line 44 through col. 6, line 9).

Taking the teachings of Saylor and Kung as a whole, it would have been obvious to one of ordinary skill in the art to incorporate the cable head-end (115 of fig. 1) through the first network (112 of fig. 1) by the hybrid-fiber-coaxial network (col.5, line 44 through col. 6, line 9) of Kung into the networks of Saylor for enhancing the functionality of components in the broadband network. Doing so would allow the system to provide ease of maintenance, control, and re-configuration as well as a reduction in cost due to shared functionality.

2. Claims 57-58 and 60-61- The cited prior art does disclose the specific claimed pathway for transmission of alarm notification to security system sever.

The appellant argues that Saylor does not teach (1) a security gateway "configured to transfer to the security system server alarm information consisting of a first notification of the alarm condition and the Alarm Video through the first network in substantially real time," (2) with the security gateway also "configured to transfer to the monitoring center a second notification of the alarm condition without transferring the Alarm Video through the second network," and (3) "the monitoring center configured to transfer to the security system server a third notification of the alarm condition."

The examiner strongly disagrees with the appellant. It is submitted that Saylor teaches a security system (fig. 1) comprising: a security gateway located at a premises (110, 120, 112, 122, 114, 124 of fig. 1), wherein the security gateway is operable to detect an alarm condition and to record video of at least a portion of the premises relating to the alarm condition, the video hereinafter referred to as an Alarm Video; security system server (130 of fig. 1) operatively coupled to the security gateway through a first network, wherein the security gateway is configured to transfer to the security system server alarm information consisting of a first notification of the alarm condition and the Alarm Video through the first network in substantially real time and wherein the security system server is remotely located relative to the security gateway (Note the connections between the security server and the property would obviously be considered as a first network, see 110, 130 of fig. 1)); a monitoring center (160 of fig. 1) operatively coupled to said security gateway through a second network (150 of fig. 1), wherein the security gateway is configured to transfer to the monitoring center a second notification of the alarm condition through the second network, wherein the monitoring center (160 of fig. 1) is remotely located relative to the security gateway and the security system server

and wherein the monitoring center is further operably coupled to the security system server (130 of fig. 1); and wherein the monitoring center is configured to transfer to the security system server a third notification of the alarm condition (160 of fig. 1); wherein the monitoring center is operatively coupled to the security system server (130 of fig. 1) through a third network (152 of fig. 1) and wherein the monitoring center is configured to transfer to the security system server the third notification of the alarm condition through the third network; Saylor further teaches wherein the security system gateway is configured to transfer to the security gateway the alarm information through the first network substantially simultaneously with transferring to the monitoring station the second notification of the alarm condition through the second network (col. 1, lines 5-13); wherein the monitoring center (160 of fig. 1) is operatively coupled to the security system server (130 of fig. 1) through the first network (Internet) and wherein the monitoring center is configured to transfer to the security system server third notification of the alarm condition through the first network; wherein the security system gateway (110 and 120 of fig. 1) is configured to transfer to the security gateway of the alarm information through the first network substantially simultaneously with transferring to the monitoring station the second notification of the alarm condition through the second network (col. 1, lines 5-13).

3. Claim 59-The cited prior art teaches substantially simultaneous transfer alarm from security gateway through a fist and second network.

The appellant argues that the cited prior art does not teach the security gateway transmits alarm information to the security system server "through the first network substantially simultaneously with transferring to the monitoring station the second notification of the alarm condition through the second network."

The examiner respectfully disagrees with the appellant. It is submitted that Saylor further teaches wherein the security system gateway is configured to transfer to the security gateway the alarm information through the first network substantially simultaneously with transferring to the monitoring station the second notification of the alarm condition through the second network (col. 1, lines 5-13).

4. Claims 47-49 -The cited prior art also discloses the security gateway notifying the security system server of loss of connectivity.

The appellant argues that Saylor teach nothing related to notification of loss of connectivity between the security gateway and the server.

The examiner respectfully disagrees with the appellant. It is submitted that Saylor further teaches wherein the security gateway is further configured to detect if connectivity with the security system server through the first network is lost and transfer to the security system server through the second network of the loss of connectivity through the first network (col. 6, lines 50-55); wherein the security gateway is further configured to transfer to the security system server in the event that connectivity with the security system server through the first network is lost while the security gateway is disarmed and the security gateway is armed before connectivity with the security system server through the first network is restored (col. 6, lines 21-34).

5. Claims 50-52- The cited prior art also does disclose notifying the security system server of loss of connectivity.

The appellant argues that Saylor does not teach notifying the security system server of loss of connectivity.

The examiner respectfully disagrees with the appellant. It is submitted that Saylor teaches wherein the security gateway is further configured to detect if connectivity with the security system server through the first network is lost and transfer to the security system server through the second network of the loss of connectivity through the first network (col. 6, lines 21-34).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Tung Vo/

Primary Examiner, Art Unit 2483

Conferees:

/Joseph G Ustaris/

Supervisory Patent Examiner, Art Unit 2483

/Mehrdad Dastouri/

Supervisory Patent Examiner, Art Unit 2621